US009386024B1

(12) **United States Patent**
Zaitsev et al.

(10) **Patent No.: US 9,386,024 B1**
(45) **Date of Patent: Jul. 5, 2016**

(54) **SYSTEM AND METHOD FOR DETECTING MODIFIED OR CORRUPTED EXTERNAL DEVICES**

(71) Applicant: **Kaspersky Lab AO**, Moscow (RU)

(72) Inventors: **Oleg V. Zaitsev**, Moscow (RU); **Olga E. Domke**, Moscow (RU); **Konstantin Y. Manurin**, Moscow (RU); **Mikhail A. Levinsky**, Moscow (RU)

(73) Assignee: **AO Kaspersky Lab**, Moscow (RU)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **14/855,442**

(22) Filed: **Sep. 16, 2015**

(30) **Foreign Application Priority Data**

Jun. 30, 2015 (RU) 2015125967

(51) **Int. Cl.**

H04L 9/00	(2006.01)
G06F 11/00	(2006.01)
H04L 29/06	(2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/105*** (2013.01); ***H04L 63/145*** (2013.01)

(58) **Field of Classification Search**
CPC . H04L 63/20; H04L 63/1416; H04L 63/1425; H04L 63/1433; H04L 63/1441; H04L 63/145; H04L 63/1458; H04L 63/1466; H04L 63/1475; H04L 63/1483
USPC 726/1, 22–26; 713/187–188
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,080,250 B2 *	7/2006	Calvert	G06F 21/568 713/168
7,257,737 B2	8/2007	Dun et al.	
7,359,962 B2 *	4/2008	Willebeek-LeMair	H04L 29/06 709/223
8,006,302 B2 *	8/2011	Abeni	H04L 63/1408 726/22

(Continued)

FOREIGN PATENT DOCUMENTS

EP	1971102 A1	9/2008
RU	2163730 C1	2/2001

OTHER PUBLICATIONS

Nohl Karsten et al. "Bad USB—On accessories that turn evil", PacSec Applied Security Conference 2014. Nov. 12, 2014/ XP-55242973.

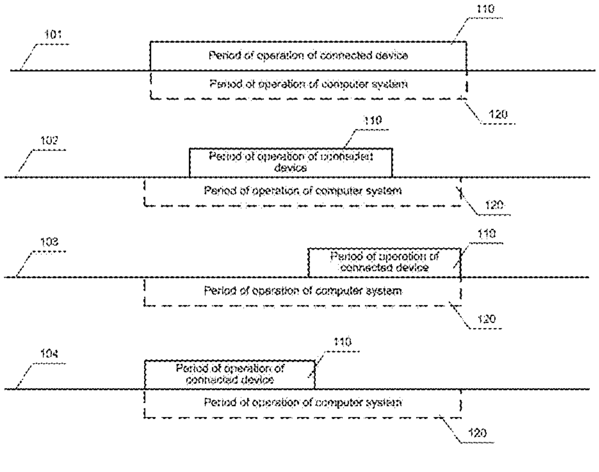
(Continued)

Primary Examiner — Hosuk Song
(74) *Attorney, Agent, or Firm* — Arent Fox LLP; Michael Fainberg

(57) **ABSTRACT**

Disclosed are systems and methods for detecting modified or corrupted external devices connected to a computer system. An exemplary method includes storing in a database, data that relates to devices previously connected to the computer system and rules that specify conditions that indicate when the device should be further analyzed as being possibly corrupted. The method further includes receiving from the device data that relates to the device or to a connection between the device and the computer system; performing an analysis of the received data by comparing the received data and the stored data relating to devices previously connected to the computer system; and applying results of the analysis of the received data to the rules to determine whether the at least one condition is satisfied that indicates that the device is possibly modified or corrupted and should be further analyzed for presence of malware.

18 Claims, 4 Drawing Sheets


110
101
Period of operation of connected device
Period of operation of computer system
120
110
102
Period of operation of connected device
Period of operation of computer system
120
110
103
Period of operation of connected device
Period of operation of computer system
120
110
104
Period of operation of connected device
Period of operation of computer system
120